



Security Assessment Report



Agora Access Control Update

October 2025

Prepared for Agora Team

Table of content

Project Summary.....	3
Project Scope.....	3
Project Overview.....	3
Findings Summary.....	4
Severity Matrix.....	4
Detailed Findings.....	5
Low Severity Issues.....	6
L-01. Executor cannot utilize eth in the contract.....	6
Informational Issues.....	7
I-01. Missing O address checks in role assignment.....	7
Disclaimer.....	8
About Certora.....	8

Project Summary

Project Scope

Project Name	Repository (link)	Commit Hash	Platform
Agora Access Control	https://github.com/amphora-atlas/contracts-dev/	4f1387 (initial commit) bf8e9db (fix commit)	Solidity

Project Overview

This document describes the manual code review findings of **Agora Access Control Update**. The following contract list is included in our scope:

- `src/contracts/access-control/AgoraAccessControl.sol`
- `src/contracts/access-control/AgoraAccessControlWithExecutor.sol`

The work was undertaken from **September 29, 2025**, to **October 13, 2025**. During this time, Certora's security researchers performed a manual audit of all the Solidity contracts and discovered several bugs in the codebase, which are summarized in the subsequent section.

Protocol and Scope Overview

Agora issues AUSD, a fiat-backed stablecoin fully collateralized by USD reserves. AUSD supports on-chain transfers across multiple networks using LayerZero for cross-chain interoperability.

AgoraAccessControl is the project's role-management module that provides enumerable, string-named roles and membership tracking used across Agora contracts.

This update requires roles to be explicitly created before they can be assigned, preventing accidental role creation due to typos. It adds create/remove helpers and emits role assignment events as before, and introduces safety checks so a role with existing members cannot be deleted. These changes tighten governance ergonomics and reduce risk of accidental misconfiguration when granting or revoking roles

Findings Summary

The table below summarizes the findings of the review, including type and severity details.

Severity	Discovered	Confirmed	Fixed
Critical	-	-	-
High	-	-	-
Medium	-	-	-
Low	1	1	1
Informational	1	1	-
Total	2	2	1

Severity Matrix

Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
Likelihood				

Detailed Findings

ID	Title	Severity	Status
L-01	Executor cannot utilize eth in the contract	Low	Fixed
I-01	Missing 0 address checks in role assignment	Informational	Acknowledged

Low Severity Issues

L-01. Executor cannot utilize eth in the contract

Severity: **Low**

Impact: **Low**

Likelihood: **Low**

Files:
AgoraAccessControlWithExecutor.sol

Status: Fixed

Description: The Executor contract implements an execute function that forwards calls to a target address. This function also always calls with `msg.value` as the value of the call. The issue is that this prevents the contract from utilizing any ETH or native token already present in the contract.

One instance where eth can accumulate in the contract if this function is used to forward send calls to the cross-chain Agora OFT token. Crosschain sends via layerzero need to be paid for with eth, which can then be refunded if in excess to the caller. If such cross-chain send calls are used and the default refund address is used (`msg.sender`), eth can accumulate in this executor contract with no way of rescuing or utilizing it.

Recommendations: Consider allowing the value to be specified by the caller. This would not increase any theft risk since the caller already needs to be an admin due to a check already present.

Customer's response: Fixed following recommendations in [PR](#).

Fix Review: Fix looks good.

Informational Issues

I-01. Missing 0 address checks in role assignment

File: AgoraAccessControl.sol

Description: When assigning roles, the `_assignRole` function does not check if the target address is a non-zero address. This allows roles to be assigned to the 0 address as well.

Recommendations: Consider adding a non-zero address check when assigning roles.

Customer's response: Acknowledged.

Disclaimer

Even though we hope this information is helpful, we provide no warranty of any kind, explicit or implied. The contents of this report should not be construed as a complete guarantee that the contract is secure in all dimensions. In no event shall Certora or any of its employees be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with the results reported here.

About Certora

Certora is a Web3 security company that provides industry-leading formal verification tools and smart contract audits. Certora's flagship security product, Certora Prover, is a unique SaaS product that automatically locates even the most rare & hard-to-find bugs on your smart contracts or mathematically proves their absence. The Certora Prover plugs into your standard deployment pipeline. It is helpful for smart contract developers and security researchers during auditing and bug bounties.

Certora also provides services such as auditing, formal verification projects, and incident response.